UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/812,607	03/30/2004	Michael Roeder	200313511-1	3195

22879 7590 10/16/2009

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
3404 E. Harmony Road
Mail Stop 35
FORT COLLINS, CO 80528

EXAMINER	
WRIGHT, BRYAN F	

ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
10/16/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
ipa.mail@hp.com
jessica.l.fusek@hp.com

Office Action Summary	Application No.	Applicant(s)	
	10/812,607	ROEDER ET AL.	
	Examiner	Art Unit	
	BRYAN WRIGHT	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 June 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6,10-30,32 and 35-58* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6, 10-30, 32, and 35-58* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

FINAL ACTION

1. This action is in response to Amendment filed 6/30/2009. Claims 49 and 50 are amended. Claims 1-6, 10-30, 32, and 35-58 are pending.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

2. Claims 1-6, 10, 12, 16-19, 25-30, 32, 36, 40-43, and 50-58 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Krohn (US Patent Publication No. 2004/0236965) and Balfanz et al. (US Patent No. 7,392,387 and Balfanz hereinafter) in view of Dondeti et al. (US Patent No. 6,263,435 and Dondeti

hereinafter) and further in view of Palekar et al. (US Patent Publication 2003/0226017 and Palekar hereinafter).

3. As to claim 1, Krohn teaches a method of secure information distribution between nodes, the method comprising: Performing, by the first node a handshake (i.e., "hello message) process with the adjacent node (i.e., intermediate node) to determine (i.e., authorization) membership in a secure group (i.e., Krohn teaches sending a handshake message to a intermediate node (e.g. Identity provide) [Steps 1-8, fig.7].

Krohn does not expressly teach distributing secure information from the first node to the adjacent node.

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Krohn as introduced by Balfanz. Balfanz discloses: distributing secure information from the first node to the adjacent node (for the purpose of distributing secure information Balfanz provides for the securing device sends to the new member the new member certificate, the group root certificate, and any necessary supporting information about the group such that the new member can now establish communication with other group members [col. 8, lines 50-67]).

Therefore, given the teachings of Balfanz, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying

Krohn by employing the well known feature of providing essential component values to handshaking disclosed above by Balfanz, for which providing group membership to neighboring devices will be enhanced [col. 8, lines 50-67].

Krohn in view of Balfanz does not expressly teach: if the adjacent node is proven to be a member of the secure group. However, these features are well known in the art and would have been an obvious modification of the system disclosed by the combination of Krohn and Balfanz as introduced by Dondeti. Dondeti discloses:

if the adjacent node is proven to be a member of the secure group (to provide the capability to determine group membership [col. 5, lines 10-30]).

Therefore, given the teachings of Dondeti, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying the combination of Krohn and Balfanz by employing the well known feature of membership validation disclosed above by Dondeti, for which providing group membership to neighboring devices will be enhanced [col. 5, lines 10-30].

Krohn and Balfanz does not expressly teach the claim limitation elements of: providing by a first node, a component value A1;

providing by an adjacent node, a component value B1 as a challenge to the first node; and wherein the handshake process comprises requiring each of the first node and the adjacent node to calculate identical values by applying the component values

A1 and B1, and a key value associated with the secure group to a one way function F(X).

However, these features are well known in the art and would have been an obvious modification of the system disclosed by the combination of Krohn, Balfanz and Dondeti as introduced by Palekar. Palekar discloses:

providing by a first node, a component value A1 (to provide a first component sending capability from a first communicating entity [par. 83]); providing by an adjacent node, a component value B1 as a challenge to the first node (to provide a second component challenge to a first communicating entity from a second communicating entity [par. 83]);

and wherein the handshake process comprises requiring each of the first node and the adjacent node to calculate identical values by applying the component values A1 and B1, and a key value associated with the secure group to a one way function F(X) (e.g., Hash) (to provide the hash function capability for authentication purposes [9O4, 9O6, fig. 9]).

Therefore, given the teachings of Palekar, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying the combination of Krohn, Balfanz and Dondeti by employing the well known feature of challenge base authentication disclosed above by Palekar, for which providing group membership to neighboring devices will be enhanced [col. 8, lines 50-67].

4. As to claim 2, Krohn teaches a method further comprising: prior to providing the secure information (i.e., first node client certificate) to the adjacent node, performing the handshake process with another adjacent node (e.g., second node) (i.e., Krohn teaches a performing a handshake with a second node. Krohn teaches sending a first node client certificate after the handshake has been confirmed with second node [par. 38 through par. 48]).

5. As to claim 3, Krohn teaches a method further comprising: Establishing (i.e., creation) an encryption key with the adjacent node (i.e., Krohn teaches he handshake allows the server to authenticate itself to the client using public key techniques, then allows the client and server to cooperate in the creation of symmetric keys used for rapid encryption, decryption and tamper detection during the session that follows [par. 105, lines 2-5]).

6. As to claim 4, Krohn teaches a method where the encryption key comprises a public key (i.e., Krohn teaches in order to establish a secure link between the two devices a protocol known as the secure socket layer (SSL) protocol is used [par. 102, lines 1-4]. Krohn teaches the SSL protocol uses a combination of public key and symmetric key encryption [par. 104, lines 1-2]).

7. As to claim 5, Krohn teaches a method where the encryption key comprises a symmetric key (i.e., Krohn teaches in order to establish a secure link between the two devices a protocol known as the secure socket layer (SSL) protocol is used [par. 102, lines 1-4]. Krohn teaches the SSL protocol uses a combination of public key and symmetric key encryption [par. 104, lines 1-2]).

8. As to claim 6, Krohn teaches a method where the secure information is distributed along with an encryption key (i.e., Krohn teaches the creation of a pre-master secret key for the security association, encrypts the pre-master secret with the server device public key and sends the encrypted pre-master secret key to the server [par. 141, lines 7-13]).

9. Claim 7, (cancelled)

10. Claim 8, (cancelled)

11. Claim 9, (cancelled)

12. As to claim 10, Krohn teaches a method where the one way function f(x) is a secure hash function (i.e., Krohn teaches a message digest can be formed by a cryptographic algorithm, a "hash function" from the message content and a secret key known to both the server and identity provider [par. 158, lines 1-3]).

13. As to claim 12, Krohn teaches a method where the secure information comprises a key for secure communication (i.e., Krohn teaches security information comprises at least one of a security certificate, at least one security key, at least one public key and at least one private key [claim 50, lines 1-5]).

14. As to claim 16, Krohn teaches a method further comprising: determining an age (i.e., inspecting) of the secure information (e.g., X.509) so that each node in the secure group will store a latest version (e.g., X.509 version number) of the secure information (i.e., Krohn teaches the presenting a X.509 certificate to a node [par. 17, lines 1-3; par. 19, line1]. The X.509 certificate inherently contains a version number for which can be checked. Krohn further teaches a intermediate node may inspect information sent [par.20, lines 1-2]).

15. As to claim 17, Krohn teaches a method where the action of determining the age of the secure information comprises: checking (i.e., inspect) a sequence number (e.g., X.509 sequence number) of the secure information (e.g., X.509) to determine the age of the secure information (i.e., Krohn teaches the presenting a X.509 certificate to a node [par. 17, lines 1-3; par. 19, line1]. The X.509 certificate inherently contains a sequence number for which can be checked. Krohn further teaches a intermediate node may inspect information sent [par.20, lines 1-2]).

16. As to claim 18, Krohn teaches a method where the action of determining the age of the secure information comprises: checking (i.e., inspect) a date of modification (i.e., validity) of the secure information (i.e., X.509) to determine the age of the secure information (i.e., Krohn teaches the presenting a X.509 certificate to a node [par. 17, lines 1-3; par. 19, line1]. The X.509 certificate inherently contains a validity field for 16. Application/Control Number: 10/812,607 Page 10 Art Unit: 2431 which validity can be check. Krohn further teaches a intermediate node may inspect information sent [par.20, lines 1-2]).

17. As to claim 19, Krohn teaches a method where the action of determining the age of the secure information comprises: checking (i.e., inspect) an elapsed time (i.e., validity) since a previous modification of the secure information (i.e., X.509) to determine the age of the secure information (i.e., Krohn teaches the presenting a X.509 certificate to a node [par. 17, lines 1-3; par. 19, line1]. The X.509 certificate inherently contains a validity field for which validity can be check. Krohn further teaches a intermediate node may inspect information sent [par.20, lines 1-2]).

18. As to claim 25, Krohn teaches an apparatus for secure information distribution between nodes, the apparatus comprising: a node configured to performing a handshake process (i.e., "hello message) with an adjacent node (i.e., intermediate node/identity provider) to determine membership (i.e., authorization) in a secure group [Steps 1-8, fig.7]).

Krohn does not expressly teach distributing secure information from the first node to the adjacent node,

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Krohn as introduced by Balfanz. Balfanz discloses:

distributing secure information from the first node to the adjacent node (for the purpose of distributing secure information Balfanz provides for the securing device sends to the new member the new member certificate, the group root certificate, and any necessary supporting information about the group such that the new member can now establish communication with other group members [col. 8, lines 50-67]).

Therefore, given the teachings of Balfanz, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Krohn by employing the well known feature of providing essential component values to handshaking disclosed above by Balfanz, for which providing group membership to neighboring devices will be enhanced [col. 8, lines 50-67].

Krohn in view of Balfanz does not expressly teach: if the adjacent node is proven to be a member of the secure group. However, these features are well known in the art and would have been an obvious modification of the system disclosed by the combination of

Krohn and Balfanz as introduced by Dondeti. Dondeti discloses: if the adjacent node is proven to be a member of the secure group (to provide the capability to determine group membership [col. 5, lines 10-30]).

Therefore, given the teachings of Dondeti, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying the combination of Krohn and Balfanz by employing the well known feature of membership validation disclosed above by Dondeti, for which providing group membership to neighboring devices will be enhanced [col. 5, lines 10-30].

Krohn and Balfanz does not expressly teach the claim limitation elements of: wherein the handshake process comprises requiring each of the first node and the adjacent node to calculate identical values by applying the component values A1 and B1, and a key value associated with the secure group to a one way function F(X).

However, these features are well known in the art and would have been an obvious modification of the system disclosed by the combination of Krohn, Balfanz and Dondeti as introduced by Palekar. Palekar discloses:

wherein the handshake process comprises requiring each of the first node and the adjacent node to calculate identical values by applying the component values A1 and B1, and a key value associated with the secure group to a one way function F(X)

(e.g., Hash) (to provide the hash function capability for authentication purposes [9O4, 9O6, fig. 9]).

Therefore, given the teachings of Palekar, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying the combination of Krohn, Balfanz and Dondeti by employing the well known feature of challenge base authentication disclosed above by Palekar, for which providing group membership to neighboring devices will be enhanced [col. 8, lines 50-67].

19. As to claim 26, Krohn teaches a apparatus (i.e., intermediate node) where the node performs the handshake process with another adjacent node, prior to providing the secure information (i.e., first node client certificate) to the adjacent node (e.g., second node) (i.e., Krohn teaches a performing a handshake with a second node. Krohn teaches sending a first node client certificate after the handshake has been confirmed with second node [par. 38 through par. 48]).

20. As to claim 27, Krohn teaches a apparatus where the node is configured to establish (i.e., creation) an encryption key with the adjacent node (i.e., Krohn teaches he handshake allows the server to authenticate itself to the client using public key techniques, then allows the client and server to cooperate in the creation of symmetric keys used for rapid encryption, decryption and tamper detection during the session that follows [par. 105, lines 2-5]).

21. As to claim 28, Krohn teaches a apparatus where the encryption key comprises a public key (i.e., Krohn teaches in order to establish a secure link between the two devices a protocol known as the secure socket layer (SSL) protocol is used [par. 102, lines 1-4]. Krohn teaches the SSL protocol uses a combination of public key and symmetric key encryption [par. 104, lines 1-2]).

22. As to claim 29, Krohn teaches a apparatus where the encryption key comprises a symmetric key (i.e., Krohn teaches in order to establish a secure link between the two devices a protocol known as the secure socket layer (SSL) protocol is used [par. 102, lines 1-4]. Krohn teaches the SSL protocol uses a combination of public key and symmetric key encryption [par. 104, lines 1-2]).

23. As to claim 30, Krohn teaches a apparatus where the secure information is distributed along with an encryption key (i.e., Krohn teaches the creation of a pre-master secret key for the security association, encrypts the pre-master secret with the server device public key and sends the encrypted pre- master secret key to the server [par. 141, lines 7-13]).

24. Claim 31, (Cancelled).

25. As to claim 32, Krohn teaches a apparatus where the one way function f(x) is a secure hash function (i.e., Krohn teaches a message digest can be formed by a cryptographic algorithm, a "hash function" from the message content and a secret key known to both the server and identity provider [par. 158, lines 1- 3]).

26. Claim 33, (Cancelled).

27. Claim 34, (Cancelled).

28. As to claim 35, although the teaching of Krohn teaches substantial features of the claimed invention, the teaching of Krohn does not disclose: An apparatus wherein the secure information comprises a password. However, these features are well known in the art and would have been an obvious modification of the system disclosed by Krohn as introduced by Palekar. Palekar discloses:

An apparatus wherein the secure information comprises a password (to provide for the capability to a password as secure information [par. 44]).

Therefore, given the teachings of Palekar, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying the combination of Krohn and Balfanz by employing the well known feature of using a secure password in challenge base authentication disclosed above by Palekar, for

which providing group membership to neighboring devices will be enhanced [904,906, fig. 9].

29. As to claim 36, Krohn teaches a apparatus where the secure information comprises a key for secure communication (i.e., Krohn teaches security information comprises at least one of a security certificate, at least one security key, at least one public key and at least one private key [claim 50, lines 1-5]).

30. As to claim 40, Krohn teaches a apparatus where the node is configured to determine (i.e. inspect) an age of the secure information (i.e., X.509 certificate) so that each node in the secure group will store a latest version of the secure information (i.e., Krohn teaches the presenting a X.509 certificate to a node [par. 17, lines 1-3; par. 19, line1]. The X.509 certificate inherently contains a version number for which can be checked. Krohn further teaches a intermediate node may inspect information sent [par.20, lines 1-2]).

31. As to claim 41, Krohn teaches a apparatus where the node is configured to check determine (i.e., inspect) a sequence number of the secure information (i.e., X.509 certificate) to determine the age of the secure information (i.e., Krohn teaches the presenting a X.509 certificate to a node [par. 17, lines 1-3; par. 19, line1]. The X.509 certificate inherently contains a sequence number for which can be checked. Krohn further teaches a intermediate node may inspect information sent [par.20, lines 1-2]).

32. As to claim 42, Krohn teaches a apparatus where the node is configured to check (i.e., inspect) a date (i.e., validity) of modification of the secure information (i.e., X.509 certificate) to determine the age of the secure information (i.e., Krohn teaches the presenting a X.509 certificate to a node [par. 17, lines 1-3; par. 19, line1]. The X.509 certificate inherently contains a validity field for which validity can be check. Krohn further teaches a intermediate node may inspect information sent [par.20, lines 1-2]).

33. As to claim 43, Krohn teaches a apparatus where the node is configured to check (i.e., inspect) an elapsed time (i.e., validity) since a previous modification of the secure information (i.e., X.509 certificate) to determine the age of the secure information (i.e., Krohn teaches the presenting a X.509 certificate to a node [par. 17, lines 1-3; par. 19, line1]. The X.509 certificate inherently contains a validity field for which validity can be check. Krohn further teaches a intermediate node may inspect information sent [par.20, lines 1-2]).

34. As to claim 49, Krohn teaches a apparatus for secure information distribution between nodes, the apparatus comprising: means performing a handshake process (i.e., "hello message) between a first node and an adjacent node (i.e., intermediate node/identity provider) to determine membership (i.e., authorization) in a secure group (i.e., Krohn teaches sending a handshake message to a intermediate node (e.g. Identity provide) [Steps 1-8, fig .7]).

Krohn does not expressly teach: wherein each of the first node and the adjacent node has an identifier value that is associated with the secure group in order for the first node and the adjacent node to have membership in the secure group; and distributing secure information from the first node to the adjacent node.

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Krohn as introduced by Balfanz. Balfanz discloses:

wherein the handshake process comprises requiring each of the first node and the adjacent node to prove a key value that is associated with the secure group (for purposes of a proving a key value in a handshake process Balfanz provides for the securing device and the potential member undertake a key exchange protocol of their choice to authenticate each other by ensuring that the public keys they use match the commitments made over the location-limited channel [col. 8, lines 34-43]);

and distributing secure information from the first node to the adjacent node (for the purpose of distributing secure information Balfanz provides for the securing device sends to the new member the new member certificate, the group root certificate, and any necessary supporting information about the group such that the new member can now establish communication with other group members [col. 8, lines 50-67]).

Therefore, given the teachings of Balfanz, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Krohn by employing the well known feature of providing essential component values to handshaking disclosed above by Balfanz, for which providing group membership to neighboring devices will be enhanced [col. 8, lines 50-67].

Krohn in view of Balfanz does not expressly teach: if the adjacent node is proven to be a member of the secure group, each of the first node and the adjacent node has an identifier value that is associated with the secure group in order for the first node and the adjacent node to have membership in the secure group.

However, these features are well known in the art and would have been an obvious modification of the system disclosed by the combination of Krohn and Balfanz as introduced by Dondeti. Dondeti discloses:

if the adjacent node is proven to be a member of the secure group (to provide the capability to determine group membership [col. 5, lines 10-30]). each of the first node and the adjacent node has an identifier value that is associated with the secure group in order for the first node and the adjacent node to have membership in the secure group (to provide group association capability utilizing a identifier value [col. 4, lines 45-57])

Therefore, given the teachings of Dondeti, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying

the combination of Krohn and Balfanz by employing the well known feature of membership validation disclosed above by Dondeti, for which providing group membership to neighboring devices will be enhanced [col. 5, lines 10-30].

Krohn and Balfanz does not expressly teach the claim limitation elements of: calculate identical values by applying a component values A1 provided by the first node, a component value B1 provided by the adjacent node, and the a key value associated with the secure group to a one way function F(X).

However, these features are well known in the art and would have been an obvious modification of the system disclosed by the combination of Krohn, Balfanz and Dondeti as introduced by Palekar. Palekar discloses:

wherein the handshake process comprises requiring each of the first node and the adjacent node to calculate identical values by applying a component values A1 provided by the first node, a component value B1 provided by the adjacent node, and the a key value associated with the secure group to a one way function F(X) (e.g., Hash) (to provide the hash function capability for authentication purposes [906, fig. 9; par. 83]).

Therefore, given the teachings of Palekar, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying the combination of Krohn, Balfanz and Dondeti by employing the well known feature of

challenge base authentication disclosed above by Palekar, for which providing group membership to neighboring devices will be enhanced [906, fig. 9; par. 83].

35. As to claim 50, Krohn teaches a apparatus for secure information distribution between nodes, the apparatus comprising: performing a handshake process (i.e., "hello message) between a first node and an adjacent node (i.e., intermediate node/identity provider) to determine membership (i.e., authorization) in a secure group (i.e., Krohn teaches sending a handshake message to a intermediate node (e.g. Identity provide) [Steps 1-8, fig .7]).

Krohn does not expressly teach: wherein each of the first node and the adjacent node has an identifier value that is associated with the secure group in order for the first node and the adjacent node to have membership in the secure group; and distributing secure information from the first node to the adjacent node.

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Krohn as introduced by Balfanz. Balfanz discloses:

wherein the handshake process comprises requiring each of the first node and the adjacent node to prove a key value that is associated with the secure group (for purposes of a proving a key value in a handshake process Balfanz provides for the securing device and the potential member undertake a key exchange protocol of their

choice to authenticate each other by ensuring that the public keys they use match the commitments made over the location-limited channel [col. 8, lines 34-43]);

and distributing secure information from the first node to the adjacent node (for the purpose of distributing secure information Balfanz provides for the securing device sends to the new member the new member certificate, the group root certificate, and any necessary supporting information about the group such that the new member can now establish communication with other group members [col. 8, lines 50-67]).

Therefore, given the teachings of Balfanz, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Krohn by employing the well known feature of providing essential component values to handshaking disclosed above by Balfanz, for which providing group membership to neighboring devices will be enhanced [col. 8, lines 50-67].

Krohn in view of Balfanz does not expressly teach: if the adjacent node is proven to be a member of the secure group, each of the first node and the adjacent node has an identifier value that is associated with the secure group in order for the first node and the adjacent node to have membership in the secure group.

However, these features are well known in the art and would have been an obvious modification of the system disclosed by the combination of Krohn and Balfanz as introduced by Dondeti. Dondeti discloses:

if the adjacent node is proven to be a member of the secure group (to provide the capability to determine group membership [col. 5, lines 10-30]). each of the first node and the adjacent node has an identifier value that is associated with the secure group in order for the first node and the adjacent node to have membership in the secure group (to provide group association capability utilizing a identifier value [col. 4, lines 45-57]).

Therefore, given the teachings of Dondeti, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying the combination of Krohn and Balfanz by employing the well known feature of membership validation disclosed above by Dondeti, for which providing group membership to neighboring devices will be enhanced [col. 5, lines 10-30].

Krohn and Balfanz does not expressly teach the claim limitation elements of: calculate identical values by applying a component values A1 provided by the first node, a component value B1 provided by the adjacent node, and the a key value associated with the secure group to a one way function F(X).

However, these features are well known in the art and would have been an obvious modification of the system disclosed by the combination of Krohn, Balfanz and Dondeti as introduced by Palekar. Palekar discloses:

wherein the handshake process comprises requiring each of the first node and the adjacent node to calculate identical values by applying a component values A1 provided by the first node, a component value B1 provided by the adjacent node, and the a key value associated with the secure group to a one way function F(X) (e.g., Hash) (to provide the hash function capability for authentication purposes [906, fig. 9; par. 83]).

Therefore, given the teachings of Palekar, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying the combination of Krohn, Balfanz and Dondeti by employing the well known feature of challenge base authentication disclosed above by Palekar, for which providing group membership to neighboring devices will be enhanced [906, fig. 9; par. 83].

36. As to claims 51, 53, 55, and 57, although the teachings of Krohn illustrates substantial features of the claim invention, Krohn does not disclose: A method where the handshake process further comprises: transmitting the calculated value between the first node and the adjacent node.

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Krohni as introduced by Palekar. Palekar discloses: A method where the handshake process further comprises: transmitting the

calculated value between the first node and the adjacent node (to provide transmitting capability of calculated hash value [par. 83]).

Therefore, given the teachings of Palekar, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Krohn by employing the well known feature of transmitting a calculated hash value disclosed above by Palekar, for which providing group membership to neighboring devices will be enhanced [par. 83].

37. As to claims 52, 54, 56 and 58, although the teachings of Krohn illustrates substantial features of the claim invention, Krohn does not disclose:

A method where the first node belongs to the secure group if the first node contains the identifier value and proves the key value during the handshake process, wherein the adjacent node belongs to the secure group if the adjacent node contains the identifier value and proves the key value during the handshake process, and wherein the secure information is distributed only between nodes in the secure group (claim 52).

An apparatus where the node belongs to the secure group if the node contains the identifier value and proves the key value during the handshake process, wherein the adjacent node belongs to the secure group if the adjacent node contains the identifier value and proves the key value during the handshake process, and wherein the secure information is distributed only between nodes in the secure group (claim 54).

An apparatus where the first node belongs to the secure group if the first node contains the identifier value and proves the key value during the handshake process, wherein the adjacent node belongs to the secure group if the adjacent node contains the identifier value and proves the key value during the handshake process, and wherein the secure information is distributed only between nodes in the secure group (claim 56).

An article of manufacture where the first node belongs to the secure group if the first node contains the identifier value and proves the key value during the handshake process, wherein the adjacent node belongs to the secure group if the adjacent node contains the identifier value and proves the key value during the handshake process, and wherein the secure information is distributed only between nodes in the secure group (claim 58).

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Krohn as introduced by Balfanz. Balfanz discloses:

A method where the first node belongs to the secure group if the first node contains the identifier value and proves the key value during the handshake process, wherein the adjacent node belongs to the secure group if the adjacent node contains the identifier value and proves the key value during the handshake process, and wherein the secure information is distributed only between nodes in the secure group (for the purpose of secure group affiliation communicating as a result of a shared

identifier and key Balfanz provides for the securing device sends to the new member the new member certificate, the group root certificate, and any necessary supporting information about the group such that the new member can now establish communication with other group members [col. 8, lines 50-67]) (claim 52).

An apparatus where the node belongs to the secure group if the node contains the identifier value and proves the key value during the handshake process, wherein the adjacent node belongs to the secure group if the adjacent node contains the identifier value and proves the key value during the handshake process, and wherein the secure information is distributed only between nodes in the secure group (for the purpose of secure group affiliation communicating as a result of a shared identifier and key Balfanz provides for the securing device sends to the new member the new member certificate, the group root certificate, and any necessary supporting information about the group such that the new member can now establish communication with other group members [col. 8, lines 50-67]) (claim 54).

An apparatus where the first node belongs to the secure group if the first node contains the identifier value and proves the key value during the handshake process, wherein the adjacent node belongs to the secure group if the adjacent node contains the identifier value and proves the key value during the handshake process, and wherein the secure information is distributed only between nodes in the secure group (for the purpose of secure group affiliation communicating as a result of a shared identifier and key Balfanz provides for the securing device sends to the new member the new member certificate, the group root certificate, and any necessary supporting

information about the group such that the new member can now establish communication with other group members [col. 8, lines 50-67]) (claim 56).

An article of manufacture where the first node belongs to the secure group if the first node contains the identifier value and proves the key value during the handshake process, wherein the adjacent node belongs to the secure group if the adjacent node contains the identifier value and proves the key value during the handshake process, and wherein the secure information is distributed only between nodes in the secure group (for the purpose of secure group affiliation communicating as a result of a shared identifier and key Balfanz provides for the securing device sends to the new member the new member certificate, the group root certificate, and any necessary supporting information about the group such that the new member can now establish communication with other group members [col. 8, lines 50-67]) (claim 58).

Therefore, given the teachings of Balfanz, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Krohn by employing the well known features of handshaking disclosed above by Balfanz, for which providing group membership to neighboring devices will be enhanced [col. 8, lines 50-67].

38. Claims 11, 13, 20, 21,35, 37, 44 and 45 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Krohn, Balfanz, Dondeli and Palekar, as

applied to claims 1 and 25, further in view of Benantar et al. (US Patent No. 6,854,056 and Benantar hereinafter).

39. As to claims 11, 13, 20 and 21, the system disclosed by the combination of Krohn, Balfanz, Dondeli and Palekar discloses substantial features of the claimed invention. However, the combination of Krohn, Balfanz, Dondeli and Palekar fails to disclose: A method where the secure information comprises a password (claim 11).

A method further comprising distributing secure information to each adjacent node that is a member of the secure group, in response to an update of the secure information (claim 13).

A method further comprising: resolving an ambiguity between a received updated secure information and currently stored secure information by selecting the secure information with a larger data value (claim 20).

A method further comprising increasing a security of the secure group by widening a secure group key (SGK) value which is known by each node in the secure group (claim 21).

However, these features are well known in the art and would have been an obvious modification of the system disclosed by the combination of Krohn, Balfanz, Dondeli and Palekar as introduced by Benantar. Benantar discloses:

A method where the secure information comprises a password (claim 11) (to provide password capability with X.509 certificate base authentication [col. 2, lines 9-12]).

A method further comprising distributing (e.g., generate) secure information to each adjacent node that is a member of the secure group, in response to an update of the secure information (claim 13) (to distribute the newly generated secure information [col. 8, lines 60-67]).

A method further comprising: resolving an ambiguity between a received updated secure information and currently stored secure information by selecting the secure information with a larger data value (claim 20) (to provide the capability to reconcile received information with stored information [col. 6, lines 45-50]).

A method further comprising increasing a security of the secure group by widening a secure group key (SGK) value which is known by each node in the secure group (claim 21) (to provide a secure group key thus enabling everyone to have the capability of trusted interaction [col. 4, lines 35-45]).

Therefore, given the teachings of Benantar, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying the combination of Krohn, Balfanz, Dondeli and Palekar by employing the well known feature of a password use in X.509 certificate-base authentication as disclosed above by Benantar, for which secure communication will be enhanced [col. 2, lines 9-12].

40. As to claims 35, 37, 44 and 45, the system disclosed by the combination of Krohn, Balfanz, Dondeli and Palekar discloses substantial features of the claimed invention. However the combination of Krohn, Balfanz, Dondeli and Palekar in view Balfanz fails to disclose:

An apparatus where the secure information comprises a password (claim 35).

An apparatus where the node is configured to distribute the secure information to each adjacent node that is a member of the secure group, in response to an update of the secure information (claim 37).

An apparatus where the node is configured to resolve an ambiguity between a received updated secure information and currently stored secure information by selecting the secure information with a larger data value (claim 44). A apparatus where the node is configured to increase a security of the secure group by widening the key value which is known by each node in the secure group (claim 45).

However, these features are well known in the art and would have been an obvious modification of the system disclosed by the combination of Krohn, Balfanz, Dondeli and Palekar as introduced by Benantar. Benantar discloses:

An apparatus where the secure information comprises a password (claim 35) (to provide password capability with X.509 certificate base authentication [col. 2, lines 9-12]).

An apparatus where the node is configured to distribute (e.g., generate) the secure information to each adjacent node that is a member of the secure group, in response to an update of the secure information (claim 37) (to distribute the newly generated secure information [col. 8, lines 60-67]).

An apparatus where the node is configured to resolve an ambiguity between a received updated secure information and currently stored secure information byselecting the secure information with a larger data value (claim 44) (to provide the capability to reconcile received information with stored information [col. 6, lines 45-50]).

An apparatus where the node is configured to increase a security of the secure group by widening the key value which is known by each node in the secure group (claim 45) (to provide a secure group key thus enabling everyone to have the capability of trusted interaction [col. 4, lines 35-45]).

Therefore, given the teachings of Benantar, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying the combination of Krohn, Balfanz, Dondeli and Palekar by employing the well known feature of a password use in X.509 certificate-base authentication as disclosed above by Benantar, for which secure communication will be enhanced [col. 2, lines 9-12].

41. Claims 14, 15, 23, 24, 38, 39, 47 and 48 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Krohn, Balfanz, Dondeli and Palekar as applied to claim 1 and 25, further in view of Haler (US Patent No. 4,530,092).

42. As to claims 14, 15, 23 and 24, the system disclosed by the combination of Krohn, Balfanz, Dondeli and Palekar discloses substantial features of the claimed invention. However, Krohn in view Balfanz fails to disclose:

A method where the action of performing the handshake process comprises: performing the handshake process with the adjacent node once for every fixed time amount T (claim 14).

A method further comprising: after detecting the presence of another node that is not in an adjacency set, attempting to handshake with that another node if a detecting node and the another node both have a handshake time remaining value of zero (0) (claim 15).

A method further comprising: allowing for rapid construction of the secure group by transmitting a burst of NB handshakes for every amount of time TB, where NB is the number of handshakes and TB is a time amount between burst of handshakes (claim 23).

A method further comprising: preventing a single node in the secure group from attempting to handshake with numerous nodes to avoid excessive joins, by establish membership with one adjacent node at a time, and waiting at time TW + TR between

handshake attempts, where TW is a fixed configurable time amount and TR is a random amount of time that is bounded by a user-specified bound range (claim 24).

However, these features are well known in the art and would have been an obvious modification of the system disclosed by the combination of Krohn, Balfanz, Dondeli and Palekar as introduced by Hafer. Hafer discloses:

A method where the action of performing the handshake process comprises: performing the handshake process with the adjacent node once for every fixed time (i.e., time slot) amount T (claim 14) (to provide time base handshaking capability [col. 9, lines 40-45]).

A method further comprising: after detecting the presence of another node that is not in an adjacency set, attempting to handshake with that another node if a detecting node and the another node both have a handshake time remaining value of zero (0) (claim 15) (to provide time base handshaking capability [col. 9, lines 40-45]).

A method further comprising: allowing for rapid construction of the secure group by transmitting a burst (e.g., broadcasting) of NB handshakes (i.e., acknowledgement) for every amount of time TB, where NB is the number of handshakes (i.e., acknowledgement) and TB is a time amount between burst (e.g., broadcasting) of handshakes (i.e., acknowledgement) (claim 23) (to provide time base handshaking capability [col. 9, lines 40-45]).

A method further comprising: preventing a single node in the secure group from attempting to handshake with numerous nodes to avoid excessive joins, by establish

membership with one adjacent node at a time, and waiting at time TW + TR (i.e., common clock signal) between handshake attempts, where TW is a fixed configurable time amount and TR is a random amount of time that is bounded by a user-specified bound range (claim 24) (to provide time slot allocation capability to communicate between adjoining nodes members [col. 9, lines 40-45].

Therefore, given the teachings of Hafer, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying the combination of Krohn, Balfanz, Dondeli and Palekar by employing the well known feature of time based acknowledgement (e.g., handshaking) and broadcasting (e.g., burst) capability disclosed above by Haler, for which secure communication will be enhanced [col. 2, lines 9-12].

43. As to claims 38, 39, 47 and 48, the system disclosed by the combination of Krohn, Balfanz, Dondeli and Palekar discloses substantial features of the claimed invention. However the combination of Krohn, Balfanz, Dondeli and Palekar fails to disclose: An apparatus where the node is configured to perform the handshake process with the adjacent node once for every fixed time amount T (claim 38).

An apparatus where the node is configured to attempt to handshake with another node if the node and the another node both have a handshake time remaining value of zero (0) (claim 39). An apparatus where the node is configured to allow for rapid construction of the secure group by transmitting a burst of NB handshakes for every

amount of time TB, where NB is the number of handshakes and TB is a time amount between burst of handshakes (claim 47).

An apparatus where the node is prevented from attempting to handshake with numerous nodes to avoid excessive joins, by establish membership with one adjacent node at a time, and waiting at time TW + TR between handshake attempts, where TW is a fixed configurable time amount and TR is a random amount of time that is bounded by a user-specified bound range (claim 48).

However, these features are well known in the art and would have been an obvious modification of the system disclosed by the combination of Krohn, Balfanz, Dondeli and Palekar as introduced by Hafer. Hafer discloses:

An apparatus where the node is configured to perform the handshake process with the adjacent node once for every fixed time (i.e., time slot) amount T (claim 38) (to provide time base handshaking capability [col. 9, lines 40-45]).

An apparatus where the node is configured to attempt to handshake with another node if the node and the another node both have a handshake time remaining value of zero (0) (claim 39) (to provide time base handshaking capability [col. 9, lines 40-45]).

An apparatus where the node is configured to allow for rapid construction of the secure group by transmitting a burst (e.g., broadcasting) of NB handshakes (i.e., acknowledgement) for every amount of time TB, where NB is the number of handshakes and TB is a time amount between burst (e.g., broadcasting) of

handshakes (claim 47) (to provide time base handshaking capability [col. 9, lines 40-45]).

An apparatus where the node is prevented from attempting to handshake with numerous nodes to avoid excessive joins, by establish membership with one adjacent node at a time, and waiting at time TW + TR (i.e., common clock signal) between handshake attempts, where TW is a fixed configurable time amount and TR is a random amount of time that is bounded by a user-specified bound range (claim 48) (to provide time slot allocation capability to communicate between adjoining nodes members [col. 5, lines 19-27]).

Therefore, given the teachings of Haler, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying the combination of Krohn, Balfanz, Dondeli and Palekar by employing the well known feature of time based acknowledgement (e.g., handshaking) and broadcasting (e.g., burst) capability disclosed above by Haler, for which secure communication will be enhanced [col. 9, lines 40-45]].

44. Claims 22 and 46 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Krohn, Balfanz, Dondeli and Palekar, as applied to claim 1 and 25, further in view of Levine et al. (US Patent Publication No. 2003/0061481 and Levine hereinafter).

45. As to claims 22 and 46, the system disclosed by the combination of Krohn, Balfanz, Dondeli and Palekar discloses substantial features of the claimed invention. However, Krohn in view Balfanz fails to disclose:

A method further comprising: decreasing an amount of time between symmetric key regeneration (TK) to increase the security of the secure group (claim 22).

A apparatus where the node is configured to decrease an amount of time between symmetric key regeneration (TK) to increase the security of the secure group (claim 46).

However, these features are well known in the art and would have been an obvious modification of the system disclosed by the combination of Krohn, Balfanz, Dondeli and Palekar as introduced by Levine. Levine discloses:

A method further comprising: decreasing an amount of time between symmetric key regeneration (TK) to increase the security of the secure group (claim 22) (to increase security between nodes by allocating symmetric keys for each node for which symmetric key regeneration is decrease [par. 65, lines 1-16]).

A apparatus where the node is configured to decrease an amount of time between symmetric key regeneration (TK) to increase the security of the secure group (claim 46) (to increase security between nodes by allocating symmetric keys for each node for which symmetric key regeneration is decrease [par. 65, lines 1-16]).

Therefore, given the teachings of Levine, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying the combination of Krohn, Balfanz, Dondeli and Palekar by employing the well known feature of symmetric key allocation for each node disclosed above by Levine, for which symmetric key processing will be enhanced [par. 65, lines 1-16].

Response to Arguments

Applicant's Remarks 35 USC 112 2nd Paragraph Rejection –Claims 49 and 50

The Examiner withdraws the rejection made under 35 USC 112, 2nd paragraph, in view of applicant's amendment to claims 49 and 50.

Applicant's Remarks 35 USC 103 Rejection –Claims 49 and 50

With regards to applicant alleging deficiently on the part of Palekar as it pertains to the ability to "apply three values to a one way function (e.g., a hash function)".

The Examiner respectfully establishes that applicant expresses recognition of the fact that Palekar's teachings do provide the capability to apply a hash function within an authentication protocol between communicating network entities. Also, Examiner respectfully establishes that applicant further recognizes that Palekar expressly discloses two parameters in the hash function. See applicant's remarks page 17 present on 6/30/2009.

The basis of applicant's argument as understood by Examiner is Palekar's alleged inability to provide teachings relative to a three parameter hash function. The

Examiner respectfully draws applicant's attention to Palekar, column 22, lines 5-10 where Palekar discloses the following, "…to provide greater security, MS-CHAP V2 also provides for the use of additional inputs into the hash function". The Examiner respectfully submits that the additional inputs as described by Palekar here are in addition to the two parameter hash Palekar has already disclosed and that applicant has formally recognized. Palekar further defines the "additional inputs" to the two parameter hash function to be additional challenge information (e.g., piggy-backed challenge) [Palekar: col. 22, lines 45-47]. The Examiner contends the applicant has not constrained the value of "A1" , citing applicant's original disclosure paragraphs 33 and 34, where applicant's states that the one-way function parameter B1 is equivalent to a challenge, and that one-way function parameter A1 is of type "value". Therefore under the broadest reasonable interpretation of possible values for "A1", the Examiner contends Palekar's addition of a "piggy-backed challenge" hash parameter for enhanced security purposes could easy be interpreted as being equivalent to applicant's hash parameter "A1".

With regards to applicant's remarks of, "… there is no reference anywhere in Palekar to a key value associated with the secure group, let alone that value being included as an input along with the two component values into the one way function as recited in claim 1", the Examiner contends applicant's disclosure support for this argument reads, "…. Authentication values are generated by sending the SGK value combined with other values by use of a one way function".

The Examiner respectfully submits that consistent with applicant's above remarks and applicant's cited disclosure are the teachings of Palekar, which discloses, "Alternatively, a key-hash can be used where the shared secret is the key used to hash an element of data" [Palekar: col. 8, lines 35-52]. The Examiner respectfully submits that those skilled in the art would recognize Palekar's teachings as cited above to be equivalent to those of applicant's with regard to sharing key information between communicating network entities and therefore the Examiner finds applicant's remarks to be non-persuasive.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRYAN WRIGHT whose telephone number is (571)270-3826. The examiner can normally be reached on 8:30 am - 5:30 pm Monday -Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on (571) 272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BRYAN WRIGHT/
Examiner, Art Unit 2431

/William R. Korzuch/
Supervisory Patent Examiner, Art Unit 2431